07-12-00 A

Practitioner's Docket No. DSC-003 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

NEW APPLICATION TRANSMITTAL

Transmitted herewith for filing is the patent application of

Inventor(s): Eugene Amdur; Irving Reid; C. Harald Koch; Steven Lamb

For (title): **GENERATION AND USE OF DIGITAL SIGNATURES**

1. Type of Application

This transmittal is for an original (nonprovisional) application.

CERTIFICATION UNDER 37 C.F.R. SECTIONS 1.8(a) AND 1.10*
*(When using Express Mail, the Express Mail label number is **mandatory**;*
Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

[ ] deposited with the United States Postal Service in an envelope addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.
37 C.F.R. Section 1.8(a)

[ ] with sufficient postage as first class mail.

37 C.F.R. Section 1.10*

[X] as "Express Mail Post Office to Address" Mailing Label No. EL504225087US (**mandatory**)

TRANSMISSION

[ ] transmitted by facsimile to the Patent and Trademark Office (703) ___-____.

Date: 7-11-2000

Signature

Ralph E. Jocke
(*type or print name of person certifying*)

WARNING:* *Each paper or fee filed by "Express Mail" **must have the number of the "Express Mail" mailing label placed thereon prior to mailing. 37 C.F.R. Section 1.10(b).*
*"Since the filing of correspondence under [Section] 1.10 without the Express Mail mailing label thereon is an oversight that can be avoided by the exercise of reasonable care, requests for waiver of this requirement will **not** be granted on petition." Notice of Oct. 24, 1996, 60 Fed. Reg. 56,439, at 56,442.*

2. Papers Enclosed

A. Required for filing date under 37 C.F.R. 1.53(b) (Regular) or 37 C.F.R. 1.153 (Design) Application

12 Page(s) of Specification
7 Page(s) of Claims
2 Sheet(s) of Drawing(s)--Informal

B. Other Papers Enclosed

3 Page(s) of declaration and power of attorney
1 Page(s) of abstract
9 Page(s) of Small Entity Statements, Assignment with Cover Sheet

3. Declaration or Oath

Enclosed

Executed by:
* inventors.

4. Inventorship Statement

The inventorship for all the claims in this application is the same.

5. Language

English

6. Assignment

An assignment of the invention to Nevex Software Technologies, Inc. is attached. A separate FORM PTO 1595 is also attached.

7. Fee Calculation (37 C.F.R. Section 1.16)

Regular Application

CLAIMS AS FILED						
Claims	Number Filed	Basic Fee Allowance	Number Extra		Rate	Basic Fee 37 CFR 1.16(a) $690.00
Total Claims (37 CFR 1.16(c))	16	- 20 =	0	x	$18.00	$0.00
Independent Claims (37 CFR 1.16(b))	4	- 3 =	1	x	$78.00	$0.00
Multiple Dependent Claim(s), if any (37 CFR 1.16(d))				+	$260.00	$0.00

Filing Fee Calculation $768.00

8. Small Entity Statement(s)

Statements that this is a filing by a small entity under 37 C.F.R. Sections 1.9 and 1.27 are attached.

Filing Fee Calculation (50% of above) $384.00

9. Fee Payment Being Made at This Time

Enclosed

Filing Fee $384.00

Recording assignment ($40; 37 C.F.R. Section 1.21(h)) (See attached "COVER SHEET FOR ASSIGNMENT ACCOMPANYING NEW APPLICATION".)	$40.00
Total Fees Enclosed	$424.00

10. Method of Payment of Fees

Charge Account No. 10-0637 (Walker & Jocke) in the amount of $424.00.
A duplicate of this transmittal is attached.

11. Authorization to Charge Additional Fees

The Commissioner is hereby authorized to charge the following additional fees by this paper and during the entire pendency of this application to Account No. 10-0637.

37 C.F.R. Section 1.16(a), (f) or (g) (filing fees)

37 C.F.R. Section 1.16(b), (c) or (d) (presentation of extra claims)

37 C.F.R. Section 1.16(e) (surcharge for filing the basic filing fee and/or declaration on a date later than the filing date of the application)

37 C.F.R. Section 1.17(a)(1)-(5) (extension fees pursuant to SECTION 1.136(a))

37 C.F.R. Section 1.17 (application processing fees)

12. Instructions as to Overpayment

Credit Account No. 10-0637 (Walker & Jocke).

Date: 7-11-2000

Ralph E. Jocke
Registration No. 31,029
Walker & Jocke
231 South Broadway
Medina, OH 44256
US
330-721-0000

Practitioner's Docket No. *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patentee: Eugene Amdur, et al.
Serial No.:
Filed on:
Title: GENERATION AND USE OF DIGITAL SIGNATURES

STATEMENT CLAIMING SMALL ENTITY STATUS
(37 CFR 1.9(f) and 1.27(b)--SMALL BUSINESS CONCERN

I hereby state that I am an official of the small business concern empowered to act on behalf of the concern identified below:

NEVEX SOFTWARE TECHNOLOGIES INC.
36 Toronto Street, Suite 1120
Toronto, Ontario, Canada M5C 2C5

I hereby state that the above identified small business concern qualifies as a small business concern, as defined in 13 CFR 121.12, and reproduced in 37 CFR 1.9(d), for purposes of paying reduced fees to the United States Patent and Trademark Office under Sections 41(a) and (b) of Title 35, United States Code, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time, part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third-party or parties controls or has the power to control both.

I hereby state that rights under contract or law have been conveyed to, and remain with, the small business concern identified above, with regard to the invention described in the application identified above.

If the rights held by the above identified small business concern are not exclusive, each individual, concern or organization having rights in the invention is listed below* and no rights to the invention are held by any person, other than the inventor, who would not qualify as an independent inventor under 37 CFR 1.9(c), if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

Each such person, concern or organization having any rights in the invention is listed below:

No such person, concern, or organization exists.

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small business entity is no longer appropriate. (37 CFR 1.28(b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed..

Name of Person Signing	Eugene Amdur
Title of Person Signing	VP Research & Development
Address of Person Signing	135 George St. South
City of Person Signing	Toronto, Ontario, Canada

SIGNATURE  Date July 7, 2000

Practitioner's Docket No. ***PATENT***

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Eugene Amdur et al.
Serial No.:
Filed on:

Title: GENERATION AND USE OF DIGITAL SIGNATURES

STATEMENT CLAIMING SMALL ENTITY STATUS
(37 CFR 1.9(f) and 1.27(b)—INDEPENDENT INVENTOR

As a below named inventor, I hereby state that I qualify as an independent inventor, as defined in 37 CFR 1.9(c), for purposes of paying reduced fees to the United States Patent and Trademark Office under Sections 41(a) and (b) of Title 35, United States Code, to the Patent and Trademark Office, with regard to the invention described in the application identified above.

I have not assigned, granted, conveyed or licensed, and am under no obligation under contract or law to assign, grant, convey or license, any rights in the invention to any person who would not qualify as an independent inventor under 37 CFR 1.9(c), if that person had made the invention, or to any concern that would not qualify as a small business concern under 37 CFR 1.9(d), or a nonprofit organization under 37 CFR 1.9(e).

Each person, concern or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below:

[ ] no such person, concern or organization
[x] persons, concerns or organizations listed below

FULL NAME NEVEX SOFTWARE TECHNOLOGIES INC.
ADDRESS 36 Toronto Street, Suite 1120, Toronto, Ontario, Canada M5C 2C5

[ ] INDIVIDUAL
[X] SMALL BUSINESS CONCERN
[ ] NONPROFIT ORGANIZATION

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further, that these statements were

made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

Eugene Amdur Date July 7, 2000

Irving Reid Date July 7, 2000

C. Harald Koch Date July 7, 2000

Steven Lamb Date July 7, 2000

GENERATION AND USE OF DIGITAL SIGNATURES

FIELD OF THE INVENTION

The present invention is directed to an improvement in computing systems and in particular to an improvement in generating and using digital signatures for digital data.

BACKGROUND OF THE INVENTION

Where the trustworthiness of digital data is important, it is known to use digital signatures to permit authentication of the digital data. When data is transferred from a sender to a recipient, the prior art provides a mechanism for the recipient to confirm that the received data is the same as the data as it was sent. A known technique is for the sender to compute a digest of the data before it is sent. The digest, and potentially other identifying data, makes up a digital signature. The digest is encrypted using a private key generated using a public key encryption standard (for example, the RSA encryption standard) and is attached to the sent data. A party seeking to authenticate the data is able to decrypt the digital signature (the data digest) using the public portion of the public-private encryption key pair. The recipient is able to compare the decrypted digest with the data received. If the decrypted digest conforms to the data actually received then the recipient of the data has an assurance that the data is the same as what was sent.

Due to the properties of the public-private pair of keys in the public encryption standard, the recipient can be assured that the digest of the data was generated by the party having access to the private key, only. In this way, the party using the data can ensure that the data has not been tampered with after the digest was encrypted by the party holding the private key.

In such a system the sender will make available the public key portion of the public-private key pair generated by the public key encryption system. This public key will permit any user having access to the public key to decrypt the digital signature which has been generated by the use of the associated private key.

Typically, in systems such as that described above, a given public-private key pair will be valid for a certain period of time, following which a new public-private key pair is generated. To ensure that the public key remains useful during the stipulated time period, it is known to save, in a secure manner, the private key, to ensure that if the system generating data is restarted for any reason, the private key will be available for use digitally after the system is restarted.

As will be apparent, the security of this system is compromised where the private key is not securely stored. In the prior art different approaches are used, including the use of smart cards for the storage of private keys, to keep the private keys secure.

Such approaches, however, either make the private keys potentially vulnerable to breaches of security or incorporate potentially expensive and complex security mechanisms to maintain the private key in a secure manner.

It is therefore desirable to have a digital signature system in which the private key may be maintained in a secure manner without requiring complex security mechanisms.

SUMMARY OF THE INVENTION

According to one aspect of the present invention, there is provided improved generation and use of digital signatures.

According to another aspect of the invention there is provided a computer program product for use with a data forwarding computer, the computer program product including a computer usable medium having computer readable program code means embodied in the medium for generating an encrypted digital signature for authentication of target data by one or more of a set of recipient computers, the computer program product including computer readable program code means for causing the data forwarding computer to:

request a private key and an associated public key from a public key encryption system,

maintain the private key in the dynamic memory of the data forwarding computer,

maintain the public key in a database available to the set of recipient computers,

generate a digital signature for the target data,

encrypt the digital signature using the public key encryption system and the private key, and

forward the target data and the encrypted digital signature to one or more of the set of recipient computers,

whereby each of the set of recipient computers is permitted to access the public key in the database to enable the decryption of the encrypted digital signature using the public key encryption system for authentication of the target data.

According to another aspect of the invention there is provided the above computer program product that includes computer readable program code restart means for causing the data forwarding computer to request a replacement private key and an associated replacement public key, the replacement private key being maintained in the dynamic memory of the data forwarding computer and the replacement public key being maintained in the database by the data forwarding computer, the restart means being invoked on a restart of the data forwarding computer.

According to another aspect of the invention there is provided the above computer program product that includes: computer readable program code means for causing the data forwarding computer to determine an elapsed time, and computer readable program code means for causing the data forwarding computer to purge each public key in the database that has been maintained in the database for longer than the elapsed time.

According to another aspect of the invention there is provided the above computer program product that includes: computer readable program code means for causing the data forwarding computer to obtain a unique identifier, and computer readable program

code means for causing the data forwarding computer to associate the unique identifier with the target data and to forward the unique identifier with the target data.

According to another aspect of the invention there is provided the above computer program product that includes: computer readable program code means for causing the data forwarding computer to maintain the unique identifier with each public key stored in the database, whereby one of the set of recipient computers is enabled to retrieve one or more public keys from the database by specifying the unique identifier.

According to another aspect of the invention there is provided a method for generating an encrypted digital signature by a data forwarding computer, for authentication of target data by one or more of a set of recipient computers, method comprising:

the data forwarding computer:

requesting a private key and an associated public key from a public key encryption system,

maintaining the private key in the dynamic memory of the data forwarding computer,

maintaining the public key in a database available to the set of recipient computers,

generating a digital signature for the target data,

encrypting the digital signature using the public key encryption system and the private key, and

forwarding the target data and the encrypted digital signature to one or more of the set of recipient computers, and

each of the set of recipient computers receiving the target data accessing the public key in the database and decrypting the encrypted digital signature using the public key encryption system to authenticate the target data.

According to another aspect of the invention there is provided a computer program product for use with a client-server computer network, the network comprising a set of server computers and a set of client computers, the computer program product including a computer usable medium having computer readable program code means embodied in the medium for providing authentication of cookies, the computer program product including:

computer readable program code means for enabling a first one of the set of client computers communicating with a first one of the set of server computers to provide identifying data to the first one of the set of server computers,

computer readable program code means for enabling the first one of the set of server computers to request a private key and an associated public key from a public key encryption system,

computer readable program code means for causing the first one of the set of server computers to maintain the private key in a dynamic memory device,

computer readable program code means for causing the first one of the set of server computers to maintain the public key in a database available to the set of server computers,

computer readable program code means for enabling the first one of the set of server computers to generate a cookie for the first one of the set of client computers, the cookie comprising data corresponding to the identifying data provided by the first one of the set of client computers,

computer readable program code means for causing the first one of the set of server computers to generate a digital signature for the cookie,

computer readable program code means for causing the first one of the set of server computers to encrypt the digital signature using the public key encryption system and the private key,

computer readable program code means for enabling the first one of the set of server computers to forward the cookie and the associated encrypted digital signature to the first one of the set of client computers,

computer readable program code means for enabling the first one of the set of client computers to communicate with a second one of the set of server computers, and in response, the second one of the set of server computers to request and receive the cookie and the encrypted digital signature from the first one of the set of client computers,

computer readable program code means for causing the second one of the set of server computers to retrieve the public key for the encrypted digital signature from the database and to decrypt the digital signature using the public key encryption system and the retrieved public key, and

computer readable program code means for enabling the second one of the set of server computers to use the decrypted digital signature to authenticate the cookie received from the first one of the set of client computers.

According to another aspect of the invention there is provided a method for providing authentication of cookies in a client-server computer network, the network having a set of server computers and a set of client computers, the method including the following steps:

a first one of the set of client computers communicating with a first one of the set of server computers, the first one of the set of client computers providing identifying data to the first one of the set of server computers,

the first one of the set of server computers requesting a private key and an associated public key from a public key encryption system,

the first one of the set of server computers maintaining the private key in a dynamic memory device,

the first one of the set of server computers maintaining the public key in a database available to the set of server computers,

the first one of the set of server computers generating a cookie for the first one of the set of client computers, the cookie comprising data corresponding to the identifying data provided by the first one of the set of client computers,

the first one of the set of server computers generating a digital signature for the cookie,

the first one of the set of server computers encrypting the digital signature using the public key encryption system and the private key,

the first one of the set of server computers forwarding the cookie and the associated encrypted digital signature to the first one of the set of client computers,

the first one of the set of client computers communicating with a second one of the set of server computers, and in response, the second one of the set of server computers requesting and receiving the cookie and the encrypted digital signature from the first one of the set of client computers,

the second one of the set of server computers retrieving the public key for the encrypted digital signature from the database and decrypting the digital signature using the public key encryption system and the retrieved public key,

the second one of the set of server computers using the decrypted digital signature to authenticate the cookie received from the first one of the set of client computers.

Advantages of the present invention include a computer system in which the generation and use of digital signatures relies on a public key encryption system where, according to the current invention, it is not necessary to maintain a private key outside the RAM memory of a computer.

BRIEF DESCRIPTION OF THE DRAWINGS

The preferred embodiment of the invention is shown in the drawings, wherein:

Figure 1 is a schematic diagram showing the prior art method for creating and using a digital signature.

Figure 2 is a block diagram illustrating the architecture of the preferred embodiment of the invention.

In the drawings, the preferred embodiment of the invention is illustrated by way of example. It is to be expressly understood that the description and drawings are only for the purpose of illustration and as an aid to understanding, and are not intended as a definition of the limits of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Figure 1 is a schematic diagram illustrating the generation and use of digital signatures using a public key system, according to the prior art. Figure 1 shows set of data 10, encryption mechanism 12 and decryption mechanism 14. The encryption and decryption in Figure 1 are based on a public key encryption system. It will be appreciated by those skilled in the art that the encryption mechanism 12 and decryption mechanism 14 may be the same application made available to both the party encrypting and the party decrypting, or may be different copies of the application resident on different computers. The party creating the digital signature (the sender), will create a digest 15 based on data 10. A private key 16 is used by encryption mechanism 12 to create encrypted digest 18. Data 10 and encrypted digest 18 are then sent to a recipient. In Figure 1, the portion of the schematic diagram above the dashed line represents the sender side of the system and the portion below the dash line represents the recipient side of the system.

As will be apparent to those skilled in the art, a sender and a recipient may be remote computers, may be different computers on the same local network, or may be different processes running on the same computer. Although the description of the preferred embodiment refers to senders and recipients, it will be apparent to those skilled in the art that the invention will be implemented in different applications where data is created and then later read and the trustworthiness of the data is important. For example, the data may be stored in a memory location rather than transferred between computers. As the preferred embodiment lends itself to distributed applications, the description refers to the transfer of data from a sender to a recipient.

At the recipient side, decryption mechanism 14 uses public key 20 to decrypt encrypted digest 18 to create digest 22. The data in digest 22 will be identical to the data in digest 15 if there has been no change to the digests during the transfer of the data. Public key 20 is part of the public/private key pair generated by the sender and corresponds to private key 16. The recipient is able to compare digest 22 to data 10 and if the digest and the data match there is an assurance that the data has been received in an unaltered state.

Figure 2 shows an example illustrating the architecture of the preferred embodiment of the invention in a block diagram form. In the example of the preferred embodiment shown in Figure 2, the system is implemented in a client server environment in which the server side of the system is distributed over three servers 30, 32, 34. Representative client 36 is shown, as well as database 38. An application of the preferred embodiment is the digital signature applied to "cookies" typically used in the client server internet environment. A cookie is a set of data used to identify a particular browser to a server or set of servers. The server will pass identification data to the user (or browser) in the form of a digitally signed cookie and subsequent queries to the web server (in the example of Figure 2 any one of servers 30, 32, 34) include the cookie. The cookie is used to communicate information about the user or browser to the web server. It is typical for a web server to store a user's authenticated identity in a cookie. To prevent such a cookie from being forged, duplicated or used by unauthorized users, the server incorporates a digital signature in the cookie.

It is known in the art to use a public key encryption system to ensure that the digital signature is secure. Such public key systems are well known to those in the art and include such standards as the RSA standard and the DSS standard. As will be understood by those skilled in the art, the preferred embodiment above may be implemented using an appropriate known public key encryption system. As described with reference to Figure 1, to digitally sign data in the form of a cookie, a digest of the data, typically a hash function generated based on the data in the cookie, is generated and the data digest is then encrypted.

For example, server 30 in Figure 2 generates a cookie for client 36. The cookie identifies client 36 to servers 30, 32, 34. In generating the cookie, server 30 uses information obtained from client 36 and adds a digital signature. To do so, server 30 creates a data digest for the cookie and obtains a private-public key pair pre-generated using a public key encryption system. The private part of the key pair used is often stored on disk (and

password protected) or on a smartcard. Using the private key, server 30 encrypts the data digest for the cookie. The cookie, with digital signature included, is sent to client 36 by server 30. When client 36 sends a query to web server 30, server 30 will access the cookie for client 36 (including the encrypted digital signature). Server 30 will use the public key (associated with the private key) to decrypt the data digest and compare the data digest data with the cookie data to confirm that the cookie was unmodified from what had been originally sent by server 30.

This prior art approach to digital signatures is useful in the context of the example shown in Figure 2, as well as other contexts where digital data is signed using a digital signature. As will be apparent, the security of the system depends on the security of the private key used by server 30. Typically, such a private key will be stored in a secure fashion on a disk associated with server 30, or in some other secure fashion, such as on a smart card.

In the system of the preferred embodiment, the private key used in generating the digital signature is not stored in a location external to the server. Rather, the private key in Figure 2 is maintained in the dynamic memory of server 30 (shown as private key 40 in Figure 2). The system of the preferred embodiment also includes database 38 which is shown in the example of Figure 2 as storing currently active public keys 42, 44, 46.

The system of the preferred embodiment functions by server 30 generating data (in the example above, the cookie data) and including with the data an identifier identifying the server. A public key encryption system is used to encrypt a digital signature as in the prior art. However, private key 40 is maintained in dynamic memory in server 30, only. This provides for increased security for the private key. The associated public key is stored in database 38. In the example of Figure 2, private key 40 in dynamic memory of server 30 has an associated public key 44 that is stored in database 38, which is accessible to other servers 32, 34 as well as server 30.

The decryption of the digital signature proceeds in the same manner as described above with respect to the prior art. When client 36 sends the cookie (the data and encrypted digital signature) to the server, the distributed server architecture shown in Figure 2 results in the cookie (the response as shown in Figure 2) being forwarded to any one of servers 30, 32, 34. In the example illustrated in Figure 2, the cookie is received by server 32 which accesses database 38 to retrieve public key 44. Server 32 is able to identify

public key 44 by the fact that server 30 included in the cookie sent to client 36 an identifier indicating that the cookie originated from server 30.

In the preferred embodiment, database 38 stores each of public keys 42, 44, 46 in association with an identifier indicating the server that generated the public key. This permits server 32 to locate, for example, public key 44 which corresponds to private key 40 by locating a public key in database 38 generated by server 30. Server 32 uses public key 44 to decrypt the digital signature in the cookie, and compare the decrypted data digest with the cookie data to determine whether the cookie is an authentic cookie, originally sent by server 30.

In the preferred embodiment database 38 is intended to store multiple public keys from each of servers 30, 32, 34. In the system of the preferred embodiment, when a server is restarted, the private key previously stored in dynamic memory is no longer available to the server. However, the public key matching the now unavailable private key is maintained in database 38. On restarting a server, the server will generate a new public-private key pair. The private key is maintained in the dynamic memory of the server, as described above. The new public key is then added to the list of public keys maintained in database 38. As will be apparent to those skilled in the art, database 38 may be distributed rather than a single database. The recipients of the data seeking to authenticate the data must be able to access the public key for the data and database 38 may have any implementation suitable to achieve this function.

When a digital signature is decrypted by one of servers 30, 32, 34, the server will access the set of public keys stored in database 38 for the server that has been identified in the data package to which the digital signature is attached. If the decryption is not successful with one of the stored public keys, the server selects another of that server's public keys found in the set stored in database 38 (if another one exists).

In this manner, the digital signature for the data may be decrypted given the public keys maintained in the database, while the private key used by the server is maintained only in the dynamic memory. As the dynamic memory is potentially more secure than disk memory, the preferred embodiment provides increased security for digital signatures.

To increase security, it is typical for digital signature systems to require changes to the public private key pairs used for digital signatures, after a particular time has elapsed.

The encryption keys are therefore replaced after a fixed length of time. In the terms of the example shown in Figure 2, a cookie will become invalid once a predetermined time expires. In the system of the preferred embodiment, the time-lapse mechanism may be implemented by the appropriate public key being simply removed from database 38. If a public key is not located in database 38 that successfully decrypts the digital signature, the associated cookie will not be used to identify client 36 and client 36 will be required to repeat a log-in or identification procedure to gain access to the server represented by servers 30, 32, 34 so as to carry out this time period constraint.

The above approach to digital signatures permits the private key for the signature to be securely stored while ensuring that recipients seeking to access the digital signature will have access to the public key by accessing a database of present and past public keys.

Although a preferred embodiment of the present invention has been described here in detail, it will be appreciated by those skilled in the art, that variations may be made thereto. Such variations may be made without departing from the spirit of the invention or the scope of the appended claims.

We Claim:

1. A computer program product for use with a data forwarding computer, said computer program product comprising a computer usable medium having computer readable program code means embodied in said medium for generating an encrypted digital signature for authentication of target data by one or more of a set of recipient computers, said computer program product comprising:

computer readable program code means for causing the data forwarding computer to request a private key and an associated public key from a public key encryption system,

computer readable program code means for causing the data forwarding computer to maintain the private key in the dynamic memory of the data forwarding computer,

computer readable program code means for causing the data forwarding computer to maintain the public key in a database available to the set of recipient computers,

computer readable program code means for causing the data forwarding computer to generate a digital signature for the target data,

computer readable program code means for causing the data forwarding computer to encrypt the digital signature using the public key encryption system and the private key, and

computer readable program code means for causing the data forwarding computer to forward the target data and the encrypted digital signature to one or more of the set of recipient computers,

whereby each of the set of recipient computers is permitted to access the public key in the database to enable the decryption of the encrypted digital signature using the public key encryption system for authentication of the target data.

2. The computer program product of claim 1 further comprising computer readable program code restart means for causing the data forwarding computer to request a replacement private key and an associated replacement public key, the replacement private key being maintained in the dynamic memory of the data forwarding computer and the replacement public key being maintained in the database by the data forwarding computer, the restart means being invoked on a restart of the data forwarding computer.

3. The computer program product of claim 2, further comprising:

computer readable program code means for causing the data forwarding computer to determine an elapsed time, and

computer readable program code means for causing the data forwarding computer to purge each public key in the database that has been maintained in the database for longer than the elapsed time.

4. The computer program product of claim 3 further comprising:

computer readable program code means for causing the data forwarding computer to obtain a unique identifier, and

computer readable program code means for causing the data forwarding computer to associate the unique identifier with the target data and to forward the unique identifier with the target data.

5. The computer program product of claim 4 further comprising:

computer readable program code means for causing the data forwarding computer to maintain the unique identifier with each public key stored in the database,

whereby one of the set of recipient computers is enabled to retrieve one or more public keys from the database by specifying the unique identifier.

6. A method for generating an encrypted digital signature by a data forwarding computer, for authentication of target data by one or more of a set of recipient computers, method comprising:

the data forwarding computer:

a. requesting a private key and an associated public key from a public key encryption system,

b. maintaining the private key in the dynamic memory of the data forwarding computer,

c. maintaining the public key in a database available to the set of recipient computers,

d. generating a digital signature for the target data,

e. encrypting the digital signature using the public key encryption system and the private key, and

f. forwarding the target data and the encrypted digital signature to one or more of the set of recipient computers, and

each of the set of recipient computers receiving the target data accessing the public key in the database and decrypting the encrypted digital signature using the public key encryption system to authenticate the target data.

7. The method of claim 6 further comprising the steps of the data forwarding computer responding to a restart condition by requesting a replacement private key and an associated replacement public key, maintaining the replacement private key in the dynamic memory of the data forwarding computer and maintaining the replacement public key in the database.

8. The method of claim 7, further comprising the steps the data forwarding computer determining an elapsed time, and purging each public key in the database that has been maintained in the database for longer than the elapsed time.

9. The method of claim 7 further comprising the steps of :

the data forwarding computer obtaining a unique identifier, and

the data forwarding computer associating the unique identifier with the target data and forwarding the unique identifier with the target data.

10. The method of claim 9 further comprising the steps of the computer readable program code maintaining the unique identifier with each public key stored in the database, and one of the set of recipient computers retrieving one or more public keys from the database by specifying the unique identifier.

11. A computer program product for use with a client-server computer network, the network comprising a set of server computers and a set of client computers, said computer program product comprising a computer usable medium having computer readable program code means embodied in said medium for providing authentication of cookies, said computer program product comprising:

a. computer readable program code means for enabling a first one of the set of client computers communicating with a first one of the set of server computers to provide identifying data to the first one of the set of server computers,

b. computer readable program code means for enabling the first one of the set of server computers to request a private key and an associated public key from a public key encryption system,

c. computer readable program code means for causing the first one of the set of server computers to maintain the private key in a dynamic memory device,

d. computer readable program code means for causing the first one of the set of server computers to maintain the public key in a database available to the set of server computers,

e. computer readable program code means for enabling the first one of the set of server computers to generate a cookie for the first one of the set of client computers, the cookie comprising data corresponding to the identifying data provided by the first one of the set of client computers,

f. computer readable program code means for causing the first one of the set of server computers to generate a digital signature for the cookie,

g. computer readable program code means for causing the first one of the set of server computers to encrypt the digital signature using the public key encryption system and the private key,

h. computer readable program code means for enabling the first one of the set of server computers to forward the cookie and the associated encrypted digital signature to the first one of the set of client computers,

i. computer readable program code means for enabling the first one of the set of client computers to communicate with a second one of the set of server computers, and in response, the second one of the set of server computers to request and receive the cookie and the encrypted digital signature from the first one of the set of client computers,

j. computer readable program code means for causing the second one of the set of server computers to retrieve the public key for the encrypted digital signature from the database and to decrypt the digital signature using the public key encryption system and the retrieved public key, and

k. computer readable program code means for enabling the second one of the set of server computers to use the decrypted digital signature to authenticate the cookie received from the first one of the set of client computers.

12. The computer program product of claim 11, further comprising:

a. computer readable program code means for assigning a unique server identifier to each one of the set of server computers,

b. computer readable program code means for associating a corresponding server identifier with each public key maintained in the database, and

c. computer readable program code means for retrieving public keys in the database by reference to a server identifier.

13. The computer program product of claim 11 further comprising computer readable program code means for removing one or more public keys from the database when the one or more public keys have been maintained in the database for longer than a preselected time.

14. A method for providing authentication of cookies in a client-server computer network, the network comprising a set of server computers and a set of client computers, the method comprising the following steps:

a. a first one of the set of client computers communicating with a first one of the set of server computers, the first one of the set of client computers providing identifying data to the first one of the set of server computers,

b. the first one of the set of server computers requesting a private key and an associated public key from a public key encryption system,

c. the first one of the set of server computers maintaining the private key in a dynamic memory device,

d. the first one of the set of server computers maintaining the public key in a database available to the set of server computers,

e. the first one of the set of server computers generating a cookie for the first one of the set of client computers, the cookie comprising data corresponding to the identifying data provided by the first one of the set of client computers,

f. the first one of the set of server computers generating a digital signature for the cookie,

g. the first one of the set of server computers encrypting the digital signature using the public key encryption system and the private key,

h. the first one of the set of server computers forwarding the cookie and the associated encrypted digital signature to the first one of the set of client computers,

i. the first one of the set of client computers communicating with a second one of the set of server computers, and in response, the second one of the set of server computers requesting and receiving the cookie and the encrypted digital signature from the first one of the set of client computers,

j. the second one of the set of server computers retrieving the public key for the encrypted digital signature from the database and decrypting the digital signature using the public key encryption system and the retrieved public key,

k. the second one of the set of server computers using the decrypted digital signature to authenticate the cookie received from the first one of the set of client computers.

15. The method of claim 14 comprising the further steps of:

a. assigning a unique server identifier to each one of the set of server computers,

b. associating a corresponding server identifier with each public key maintained in the database, and

c. retrieving public keys in the database by reference to a server identifier.

16. The method of claim 14 comprising the further step of removing one or more public keys from the database when the one or more public keys have been maintained in the database for longer than a preselected time.

ABSTRACT

A digital signature is generated in association with target data. The computer generating the digital data encrypts the digital signature using a public key encryption system. The private key is stored in dynamic memory in a secure manner. The public key associated with the private key is stored in an accessible database. The public key is accessed from the database and used by recipient computers to authenticate the target data by decrypting the encrypted digital signature. When the computer generating the digital signature is restarted, the private key stored in dynamic memory is lost. The computer obtains a new private and public key pair from the public key encryption system. The previously used public key is maintained in the database until a predefined time has elapsed, after which it is removed from the database.

Fig. 1
(Prior Art)

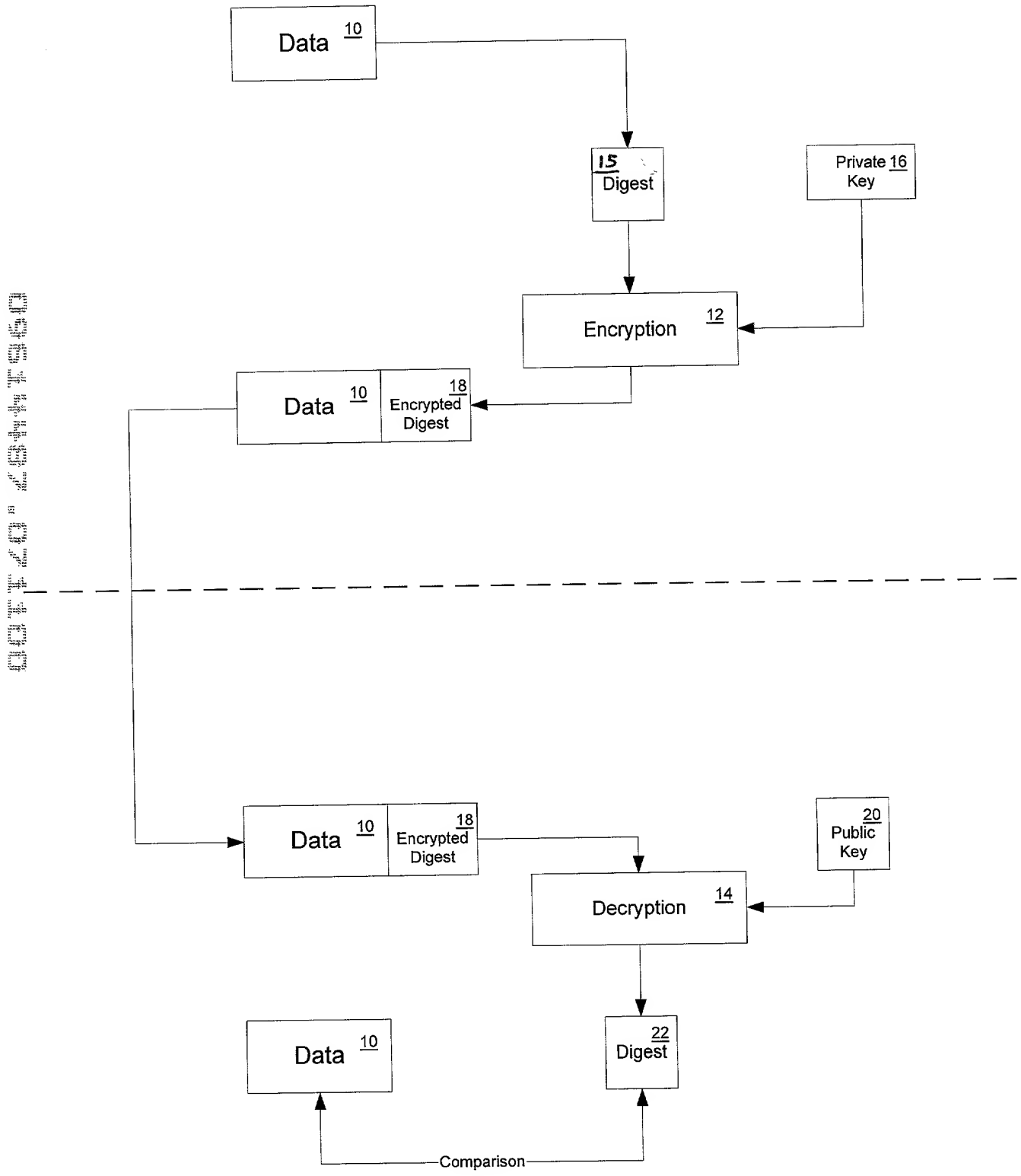
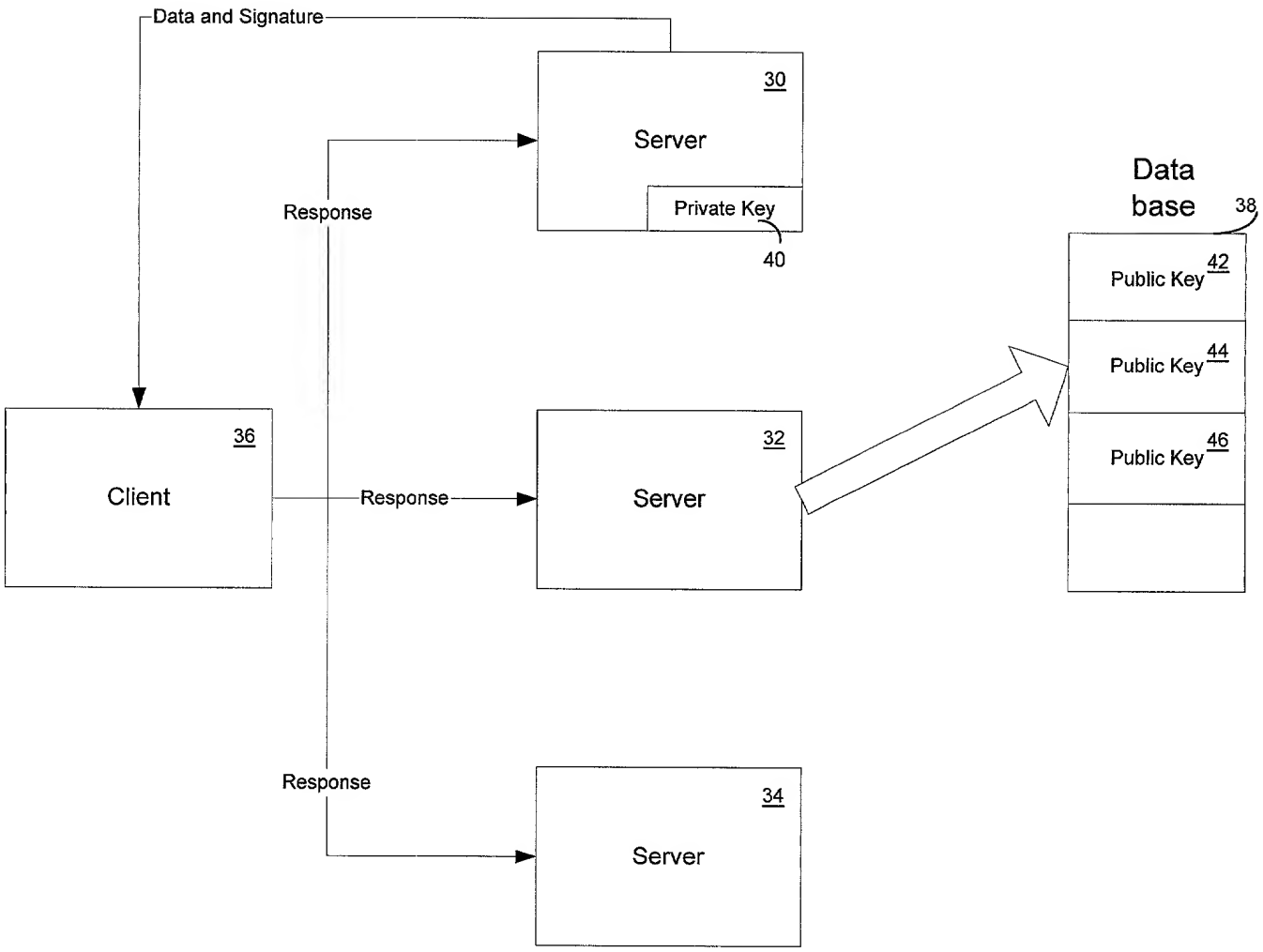


Fig. 2


Data and Signature
30
Server
Private Key
40
Response
Data base
38
Public Key 42
Public Key 44
Public Key 46
36
Client
Response
32
Server
Response
34
Server

Practitioner's Docket No. *PATENT*

COMBINED DECLARATION AND POWER OF ATTORNEY

(ORIGINAL, DESIGN, NATIONAL STAGE OF PCT, SUPPLEMENTAL, DIVISIONAL, CONTINUATION, OR C-I-P)

As a below named inventor, I hereby declare that:

TYPE OF DECLARATION

This declaration is for an original application.

INVENTORSHIP IDENTIFICATION

My residence, post office address and citizenship are as stated below, next to my name. I believe that I am an original, first and joint inventor of the subject matter that is claimed, and for which a patent is sought on the invention entitled:

TITLE OF INVENTION

GENERATION AND USE OF DIGITAL SIGNATURES

SPECIFICATION IDENTIFICATION

The specification is attached hereto.

ACKNOWLEDGMENT OF REVIEW OF PAPERS AND DUTY OF CANDOR

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information, which is material to patentability as defined in 37, Code of Federal Regulations, § 1.56.

PRIORITY CLAIM

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):			Priority Claimed
_____ (number)	_____ (country)	_____ (date filed)	( ) ( ) yes no
_____ (number)	_____ (country)	_____ (date filed)	( ) ( ) yes no
_____ (number)	_____ (country)	_____ (date filed)	( ) ( ) yes no

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose material information as defined by Title 37, Code of Federal Regulations, Section 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

_____ (Appln. Serial No.)	_____ (Filing Date)	_____ (Status: patented, pending, abandoned)

POWER OF ATTORNEY

I hereby appoint the following practitioner(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

David R. Percio	Registration Number 30,096
Ralph E. Jocke	Registration Number 31,029

I hereby appoint the practitioner(s) associated with the Customer Number provided below to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

SEND CORRESPONDENCE TO

Ralph E. Jocke
Walker & Jocke, L.P.A.
231 South Broadway
Medina, OH 44256

Customer Number IDON301265

DIRECT TELEPHONE CALLS TO:

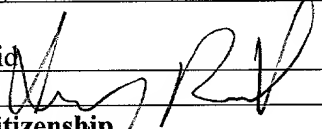
Ralph E. Jocke
(330) 721-0000

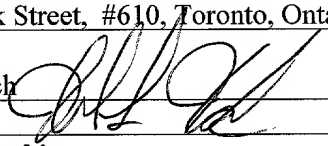
DECLARATION

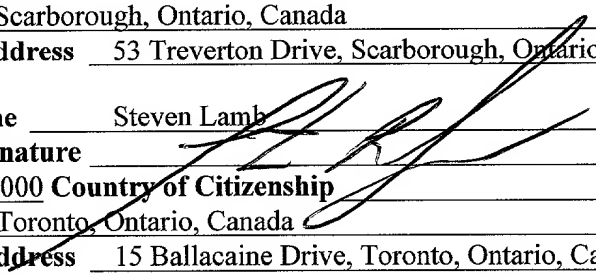
I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURE(S)

Inventor Name Eugene Amdur
Inventor's signature 
Date July 7, 2000 **Country of Citizenship** Canadian
Residence Toronto, Ontario Canada
Post Office Address 135 George Street South, #704, Toronto, Ontario, Canada M4A 4E8

Inventor Name Irving Reid
Inventor's signature 
Date July 7, 2000 **Country of Citizenship** Canadian
Residence Toronto, Ontario, Canada
Post Office Address 152 St. Patrick Street, #610, Toronto, Ontario, Canada M5T 3J9

Inventor Name C. Harald Koch
Inventor's signature 
Date July 7, 2000 **Country of Citizenship** Canadian
Residence Scarborough, Ontario, Canada
Post Office Address 53 Treverton Drive, Scarborough, Ontario, Canada M1K 3S5

Inventor Name Steven Lamb
Inventor's signature 
Date July 7, 2000 **Country of Citizenship** Canadian
Residence Toronto, Ontario, Canada
Post Office Address 15 Ballacaine Drive, Toronto, Ontario, Canada M8Y 4A7